Lions Clube de Vila Franca do Campo organizam Festa das Vindimas

O Lions Clube de Vila Franca organiza, mais uma vez, a tradicional Festa das Vindimas, um marco da sua actividade lionística por permitir angariar fundos para as diferentes acções realizadas durante o ano lionístico, com o objectivo primeiro de Servir a população Vila Franquense.

Assim, no dia 22 de Outubro, no pavilhão AçorArena, pelas 13 horas, será possível testemunhar o envolvimento e participação activa de todos os sócios do Clube para proporcionarem aos presentes uma almoço convívio, de sabores tradicionais, em que o companheirismo, a confraternização e a boa disposição são apanágio.

Ordenados dois novos diáconos na festa da Imaculada Conceição

A partir do dia 8 de Dezembro, a Diocese de Angra passa a ter dois novos diáconos que serão ordenados presbíteros no final do ano pastoral de 2016/2017, numa celebração que regressará ao santuário de Nossa Senhora da Conceição dois anos depois.

Os seminaristas Jacob Vasconcelos e Nelson Pereira, naturais das ilhas das Flores e da Terceira, respectivamente, alunos do sexto ano do Seminário Episcopal de Angra, serão ordenados diáconos na festa da Imaculada Conceição, retomando uma tradição na diocese de Angra, interrompida há dois anos.

A ordenação dos dois diáconos culmina um conjunto de celebrações que o Santuário vive particularmente neste dia consagrado a Nossa Senhora e que começam com uma novena preparatória envolvendo grupos paroquiais e movimentos eclesiais nos diferentes dias. A pregação do novenário será feita pelo padre Tiago Tedéu, pertencente à ouvidoria da Horta.

O Santuário, que assinala o seu 28º aniversário e 13 anos da reinstalação da Confraria de Nossa Senhora da Conceição, conta agora com dois sacerdotes: o reitor, cónego Francisco Dolores e um vigário paroquial, que é o sacerdote diocesano mais novo a paroquiar nos Açores, o padre Pedro Lima.

O culto de Nossa Senhora da Conceição é um dos mais antigos em Angra do Heroísmo. A primeira igreja de Angra que lhe é dedicada é mandada construir em 1470, a Igreja de Nossa Senhora da Conceição que o sismo de 1980 haveria de destruir.

Com a reabertura do templo reconstruído, no momento em que se celebrava o Ano Episcopal Mariano, o pedido de elevação da Igreja de Nossa Senhora da Conceição a Santuário Mariano foi feito nesse mesmo ano de 1987 pelo pároco da altura, padre Adão Teixeira, benesse que foi concedida ainda no mesmo ano pelo Bispo de Angra, D. Aurélio Granada Escudeiro.

IA

Cibersegurança - a proteção da identidade online

Por: Jerónimo Nunes
Docente da Universidade dos Açores
jeronimo.am.nunes@uac.pt

A Cibersegurança tem como objetivo estudar e definir mecanismos de proteção dos computadores conectados através da Internet, das comunicações que entre eles se estabelecem e das informações armazenadas naqueles sistemas, impedindo acessos não autorizados que possam por em causa a confidencialidade, integridade e disponibilidade das informações. À semelhança do mundo real, também no mundo das redes e dos sistemas informáticos, o ciberespaço, é necessária uma identidade para que as pessoas sejam reconhecidas e distinguidas umas das outras pelos sistemas e sítios web. A "ciberidentidade", identidade virtual ou identidade online é indispensável para as pessoas acederem aos serviços públicos ou privados que são disponibilizados por sistemas informáticos através da Internet e das redes de comunicação móveis.

A identidade real (ou offline) é constituída por diversos elementos que distinguem uma pessoa das outras: nome, filiação, naturalidade, data de nascimento, morada, altura, fisionomia, impressões digitais. A esta identidade, mantida pelos serviços do Estado, são associados números de identificação (civil, fiscal, de utente de saúde e da segurança social) que estão registados num cartão de identificação, no caso português, o cartão de cidadão. A autenticidade da identidade é comprovada pela apresentação do cartão de cidadão que contém um elemento visual (fotografia) e a impressão digital. São elementos complementares e redundantes que se validam mutuamente e tornam mais difícil uma eventual falsificação. Neste processo de autenticação da identidade são usados dois tipos de elementos: uns que representam aquilo que a pessoa é - fotografia, impressão e outros aspetos físicos - outros relativos ao que a pessoa possui - nome, filiação, morada.

A identidade online identifica as pessoas perante os sistemas informáticos ou sítios web que disponibilizam serviços bancários, de seguros, da administração fiscal, da segurança social, no presente, de justiça, saúde, educação, no futuro próximo. Os sistemas de correio eletrónico (email) ou comércio eletrónico (e-commerce) também exigem uma identidade online. A identidade online é parcial, porque não identifica completamente a pessoa e contem apenas um elemento, o nome de utilizador, sendo mais vulnerável a falsificações. Uma pessoa possui normalmente várias entidades online, uma para cada um dos sistemas perante os quais necessita identificar-se para usufruir dos respetivos serviços. O nome de utilizador (username), único para cada sistema, normalmente não confidencial, é escolhido pela pessoa, como no caso de parte do endereço de email. Em outros casos, o nome de utilizador é escolhido pela entidade que disponibiliza o serviço: nº de identificação fiscal ou o nº de conta bancária. A senha (password), associada ao nome de utilizador, comprova a autenticidade deste, é confidencial e sempre escolhida pela pessoa. Neste modo de autenticação é usado um outro tipo de elemento - o que a pessoa sabe.

O furto ou usurpação da identidade online consiste em obter a senha associada ao nome de utilizador relativo a um sistema e usá-la, sem o consentimento da pessoa detentora da identidade, em prejuízo desta e em benefício do "cibercriminoso". As consequências do furto da identidade online são inúmeras e danosas: acesso (violação da privacidade), divulgação (difamação), modificação e destruição da informação relativa a vários aspetos da vida de uma pessoa. Em particular: uso da identidade online para acesso a contas bancárias, aquisição de bens ou serviços (através dos cartões de crédito) ou para fins ilícitos: desencadear ataques informáticos, executar fraudes e roubos. Muitas vezes, o furto apenas é detetado depois de produzir efeitos e será oneroso ou impossível reparar os danos provocados. Poderá ser difícil a uma pessoa provar a não responsabilidade pelo uso indevido da sua identidade online por outros.

O "cibercriminoso" (black hat hacker) recorre a vários métodos para obter as senhas: software específico que explora as senhas vulneráveis efetuando tentativas exaustivas para as descobrir ou tabelas (dicionários) com as senhas mais frequentes. Ludibriar as pessoas com mensagens forjadas (email ou SMS) e levá-las a fornecer as senhas e a observação das pessoas quando digitam as senhas nos locais de trabalho ou em lugares públicos, são outros dos estratagemas usados. A prevenção do furto da identidade online passa essencialmente por garantir a confidencialidade das senhas, escolhendo uma senha robusta e recorrendo a boas práticas no uso seguro e na preservação das senhas. Devem igualmente ser protegidos os dispositivos utilizados e as conexões às redes de comunicação. É aconselhável conhecer os sistemas e sítios web em que são usadas as identidades online e verificar se as entidades fornecedoras dos serviços oferecem confiança. As entidades gestoras dos sistemas informáticos que disponibilizam os serviços online devem também tomar medidas para impedir ataques que levem à descoberta das senhas dos utentes.

Nas boas práticas no uso da identidade online incluem-se: nunca divulgar a senha - passando de pessoa em pessoa até chegar a alguém que poderá alterá-la e usar a identidade para fins indevido; não fornecer a senha, ou qualquer elemento da identidade online, em resposta a qualquer solicitação por email (são mensagens forjadas, de phishing) porque as entidades nunca pedem as senhas aos seus utentes. A mesma senha não deve ser usada para identidades em sistemas ou sítios web distintos, embora com nomes de utilizador diferentes, porque o furto da senha comprometerá todas as identidades. Ao terminarem a interação com sistemas de correio eletrónico, redes sociais, ou outras aplicações em sítios web, devem os utilizadores efetuar "logout" ou "exit" (ou seja, fechar ou sair). Verificar se as ligações à Internet através de "hotspots" Wi-Fi públicos proporcionam comunicações seguras - se é exigida uma password - será outro procedimento a efetuar.

Os nossos computadores devem ser protegidos contra software maligno (vírus, sypware) e não devemos usar computadores ou smartphones de outras pessoas porque poderão não estar protegidos, nem permitir que outras pessoas utilizem o nosso computador ou smartphone porque poderão, mesmo não intensionalmente, comprometer a segurança. As passwords não devem ser guardadas no computador, nos browsers ou em ficheiros, mas em papel, em local não visível, afastado do computador. Ao guardar as senhas na nuvem (cloud), a sua proteção será garantida pela robustez de uma outra password - a descoberta desta afetará todas. O recurso a software gestor de senhas deverá acontecer apenas no caso de comprovada confiança.

Na definição de uma identidade online, considera-se em primeiro lugar a escolha do nome de utilizador que não deverá ser o nome próprio ou outro que dê indicações sobre a identidade real. Em alguns sistemas (da administração fiscal ou bancários) não é possível escolher o nome de utilizador e noutros é exigido um endereço de email como nome de utilizador.

Em segundo lugar, deverá ser escolhida uma senha robusta, resistente às tentativas de descoberta, de acordo com os seguintes critérios: conter 10 ou mais caracteres, não incluir nomes próprios, diminutivos ou alcunhas, palavras do dicionário, sequências de algarismos, nºs de telefone, datas de nascimento ou marcas de produtos. É aconselhável combinar maiúsculas, minúsculas, algarismos e outros símbolos usados na escrita. A senha deverá ser alterada cada 2 ou 3 meses, apesar dos sistemas não o pedirem. Como a escolha de uma senha fácil de memorizar pode não ser uma tarefa fácil de compatibilizar com uma senha difícil de descobrir, pode ser equacionado o recurso a software gerador de senhas mas apenas quando ofereça garantias de confidencialidade. Por outro lado, não devem ser usadas as senhas geradas em sites web porque quem tenta descobri-las também utilizará estes sítios. A robustez de uma senha também não deve testada em sites web - os sites podem não ser de confiança e utilizarem as senhas testadas em tentativas de furto da identidade online. Se não for possível obter uma palavra secreta (password) seguido os critérios enunciados poderá tentar-se construir uma frase secreta (passphrase).

Um dos métodos mais divulgados para construção de senhas robustas consiste em substituir numa palavra algumas vogais e consoantes por algarismos. Por exemplo, substituir as vogais o por 0 (zero), e por 3; i por 1; as consoantes b por 8; s por 5. Por ser muito divulgado, este método dever ser usado com cuidado: não efetuar substituições muito óbvias ou conhecidas, como as exemplificadas. Existem outras técnicas alternativas: intercalar sinais de pontuação ou algarismos numa palavra; ligar várias palavras curtas com sinais de pontuação; numa frase longa, retirar a primeira letra de cada palavra e intercalar com números; construir frases sem sentido que não sigam as regras gramaticais.

No acesso aos sistemas online e sítios web, a identidade pedida é por estes autenticada, mas a pessoa não verifica a autenticidade daqueles sistemas e sítios - não ocorre uma autenticação mútua (como nos serviços secretos e militares através de uma senha e contra-senha) que poderia evitar o furto da identidade. A autenticação mútua é conseguida com a troca de certificados digitais emitidos por entidades competentes. A assinatura digital autentica a identidade do autor e evita o repúdio autoria. Estes dois mecanismos de autenticação avançada estão disponíveis no cartão de cidadão.

Foto:DR